HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/843,072	04/26/2001	Rodney Carlton Burnett	AUS920010162US1	8490

7590 01/12/2005

Darcell Walker
8107 carvel Lane
Houston, TX 77036

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/843,072	BURNETT ET AL.	
	Examiner	Art Unit	
	Samson B Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims **1-28** have been examined.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. **Claims 1,13-14, 22** are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1,11-12, 20 of the copending Application No. 09/843069 (hereinafter refereed as '843 application). Although the conflicting claims are not identical, they are not patentably distinct from each other.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

- **As per claim 1, claim 1** of the instant application and claim 1 of the '843 application recite similar method for controlling access to a computing system resource except claim 1 of the instance claim is being accessed through a symbolic link file with externally stored resources and claim 1 of '843 application is being accessed through a special device file, with externally stored resources. Furthermore all elements/limitation

of claim 1 of the instant application is recited in the claim 1 of the '843 application. It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to replace or use device file instead of symbolic file for the purpose redirecting or ultimately accessing the target resource or the system device because both of them namely "symbolic link" and "Device files" are "file system Aliases" used for ultimately locating and referencing system resources as per teachings Tivoli Secure Way Policy Director for Operating Systems Administration Guide Version 3 Release 7 (hereinafter referred as **Tivoli**) (reference U) [See Page 19, reference "File System Aliases" up to page 23, reference "Device Files")

- **As per claim 13, claim 13** of the instant application and claim 11 of the '843 application recite similar method for controlling access to a computing system resource except claim 13 of the instance claim is being accessed through a symbolic link file with externally stored resources and claim 11 of '843 application is being accessed through a special device file, with externally stored resources. Furthermore all elements/limitation of claim 13 of the instant application is recited in the claim 11 of the '843 application. It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to replace or use device file instead of symbolic file for the purpose redirecting or ultimately accessing the target resource or the system device because both of them namely "symbolic link" and "Device files" are "file system Aliases" used for ultimately locating and referencing system resources as per teachings Tivoli Secure Way Policy Director for Operating Systems Administration Guide Version 3 Release 7 (hereinafter referred as **Tivoli**) (reference U) [See Page 19, reference "File System Aliases" up to page 23, reference "Device Files")

- **As per claim 14, claim 14** of the instant application and claim 12 of the '843 application recite similar limitation of computer program product in a computer

readable medium for controlling access to a computing system resources method except claim 14 of the instance claim is being accessed through a symbolic link file with externally stored resources and claim 12 of '843 application is being accessed through a special device file, with externally stored resources. Furthermore all elements/limitation of claim 14 of the instant application is recited in the claim 12 of the '843 application. It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to replace or use device file instead of symbolic file for the purpose redirecting or ultimately accessing the target resource or the system device because both of them namely "symbolic link" and "Device files" are "file system Aliases" used for ultimately locating and referencing system resources as per teachings Tivoli Secure Way Policy Director for Operating Systems Administration Guide Version 3 Release 7 (hereinafter referred as **Tivoli**) (reference U) [See Page 19, reference "File System Aliases" up to page 23, reference "Device Files")

- **As per claim 22, claim 22** of the instant application and claim 20 of the '843 application recite similar limitation as a computer connectable to a distributed computing system, controlling access to a computing system resource except claim 22 of the instance claim included symbolic links pointing to the system resources and claim 20 of '843 application includes a special device files containing information relating to corresponding system device. Furthermore all elements/limitation of claim 22 of the instant application is recited in the claim 20 of the '843 application. It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to replace or use device file instead of symbolic file for the purpose redirecting or ultimately accessing the target resource or the system device because both of them namely "symbolic link" and "Device files" are "file system Aliases" used for ultimately locating and referencing system resources as per teachings Tivoli Secure Way Policy

Director for Operating Systems Administration Guide Version 3 Release 7 (hereinafter referred as **Tivoli**) (reference U) [See Page 19, reference "File System Aliases" up to page 23, reference "Device Files")

Specification

4. The disclosure is objected because of the following informalities:

- On page 8, lines 31, the "methods of the **present will** not apply", has been recited. There is a word missing between the word **"present"** and the word **"will"**
- On page 9, line 29-30, "the file object information for the accessed **a** resource is retrieved", has been recited. It should have been written as "the file object information for the accessed resource is retrieved"
- On page 10, lines 6-7; "If the search resulted **in** a found target resource/object, step 22, then this search result means that the security policy does protect this resource" has been recited. It should have been written as "If the search resulted **is** a found target resource/object, step 22, then this search result means that the security policy does protect this resource"

Appropriate correction is required.

Drawings

5. The drawing is objected because of the following informalities:

- Figure 6, does not contain the references that are cited on page 12, second paragraph. For instance "Boxes 50-54" have been recited however the corresponding figure 6 does not indicate all these references. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. **Claims 1-28** are rejected under 35 U.S.C. 102(a) as being anticipated by Tivoli Secure Way Policy Director for Operating Systems Administration Guide Version 3 Release 7 (hereinafter referred as **Tivoli**) (reference U)

8. **As per claims 1, 14 and 23 Tivoli discloses** a method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource [Page 1, paragraph 3 and 4; page 19, reference "File System Aliases"] comprising the steps of:

- Determining a system resource named in the symbolic link through which the access attempt is made; [Page 19, reference, "File System Aliases"] ("the system resource" is the "target resource" or "the underlying resources" pointed by the symbolic link as explained on page 9, 1st paragraph and page 10 of the

submitted disclosure by the applicant. When a system resource or the target resource named in the symbolic link or pointed by the symbolic link is accessed or searched, access to the target resource or the system resource will be determined based on the authorization policy attached to the symbolic link through which the access attempt is made as explained on Page 19, reference, "File System Aliases" up to page 22, 2nd paragraph]

- Searching a protected objects database for entries protecting said system resource and generating a list of said entries; [Page 9, paragraph 4, reference "Protected Object Policies"; page 19, reference "File System Aliases" up to page 22 second paragraph] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects. Before access is granted the protected database is searched and the governing authorization policy is determined based on the authorization policy attached or associated to these symbolic links which are pointing to the target resource as explained on page 19, last paragraph up to page 22 second paragraph).

- Generating an authorization decision for the access attempt based on security policies that govern all entries in the database protecting the system resource. [Page 9, paragraph 4, reference "Protected Object Policies"; page 19, reference "File System Aliases" up to page 22 second paragraph] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects. When these database is searched the governing authorization policy is determined based on the authorization policy attached or associated to these symbolic links which are pointing to the

target resource. The authorization decision for the access attempts is made after the security authorization policies which are attached to all entities or all symbolic links which are pointing to the target resources are checked or examined. The decision will be made accordingly after all entities or symbolic links are examined as explained on page 19, reference "File System Aliases" up to page 22 second paragraph)

9. **As per claims 13 Tivoli discloses** a method for controlling access to a computing system device being accessed through symbolic link, said access control being implemented through an externally stored resource [Page 1, paragraph 3 and 4; page 9, reference "File System Aliases"] comprising the steps of:

- Monitoring the computing system for activities related to creating and accessing symbolic links that link to system resources; [Page 19, reference "File System Aliases"- page 22 second paragraph; page 23, reference "Trusted Computing Base Resources"; page 52, reference "TCB Monitoring"]

- Restricting the creation of symbolic link files based on the rules defined in the externally stored resource/authorization policy; [Page 1, paragraph 3 and 4;Page 15-page 17; page 9 paragraph 4; page 19, reference "File System Aliases" -page 22 second paragraph]

- Restricting accesses to system resources that are linked to and accessed by a symbolic link. [page 19, reference "File System Aliases" -page 22 second paragraph]

10. **As per claims 22 Tivoli discloses** a computer connectable to a distributed computing system, which included symbolic links pointing to system resources and comprising:

- A processor; [Page 53, table "30", reference "Monitor-threads, description"]
- A native operating system; [page 2, figure 1, ref. "Native OS services"]
- Application programs; [Page 2, figure 1, ref. "PDOS"; page 74, last paragraph-page 75, first paragraph] (PDOS is an application program that is installed on each machine that is needed to be protected as explained on page 2, 1st paragraph, last line.]
- An externally stored authorization program overlaying said native operating system and augmenting the standard security controls of said native operating system; [Page 1, 3rd paragraph, under the title "understanding PDOS"]
- A protected objects database within said external authorization program containing as entries protected symbolic link files and system resources pointed to by these protected symbolic links such that the protection of the symbolic link is attached to said system resources; [Page 1, 3rd and 4th paragraph; page 2, reference "PDOS Databases"; page 9, reference "Protected Object Policies"; page 19, reference "File System Aliases" up to page 22 second paragraph]
- A decision component with said authorization program for controlling access to system resources being accessed through symbolic links; and a decision component with said authorization program for controlling the creation of symbolic links through which system resources are accessed.[Page 2, reference "PDOS DataBases" - page 3, 1st paragraph; Page 9, reference "Protected Object Policies"; page 19, last paragraph-page 22 second paragraph]

11. **As per claims 2 and 24 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 1 and 23 above. Furthermore Tivoli discloses the method wherein said control method grants access if said search does not find in the protected objects database, the system resource named in the symbolic link through which the access attempt is made. [page 9, reference "protected object Policies"; page 19, reference "File System Aliases"-page 22 second paragraph] (As explained under the title "Protected Object Policies" on page 9 and on page 19, reference "File System Aliases" up to page 22 second paragraph] objects which are required to be protected have the security authorization policy attached to them directly or through the symbolic links which are pointed to the target resources. When the access attempt is made, the protected database is searched through the symbolic links before access is granted to the target resources. This implicitly implies if said search does not find in the protected objects database, the system resource named in the symbolic link through which the access attempt is made is not protected therefore access will be granted.)

12. **As per claims 3, 15 and 25 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 1, 14 and 23 above. Furthermore Tivoli discloses the method, wherein said authorization decision step comprises the steps of: retrieving a current entry from said generated database list; calling an access decision component of the externally stored resource to obtain an access decision for the access attempt based on the security policy that governs the current entry in the generated database list; determining whether the access decision component granted access; if the decision component granted access, determining whether more entries are in this database list; and updating a current entry in said database list when more entries are in the list and returning to said current entry retrieving step.[Page 1,

paragraph 3 and 4; page 19, reference "File System Aliases"; page 19, reference "File System Aliases" up to page 22 second paragraph]

13. **As per claims 4 and 16 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 3 and 15 above. Furthermore Tivoli discloses the method further comprising the step of denying the access attempt when the decision component denies access based on the security policy for the current database entry. [Page 9, reference "protected object Policies"] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects.)

14. **As per claims 5 and 17 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 3 and 15 above. Furthermore Tivoli discloses the method further comprising the step of allowing the access attempt if no more entries are in the database list. [Page 9, reference "protected object Policies"; page 19, reference "File System Aliases" up to page 22, second paragraph] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects. The governing authorization policy could be the one which are attached on the symbolic links pointing to the target resource or the authorization policy attached to the target resources directly as explained on page 19, reference "File System Aliases" up to page 22 second paragraph. All authorization policies which are attached to the symbolic links which are pointing to the target

resources are checked before access to the target resource is granted. This implicitly implies that if there is no more entities in the protected database that are pointing to the target resource that means all the entities are already passed the authorization test and access should be allowed and this meets the recitation of the claim.)

15. **As per claims 6-8 and 18-20 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 1 and 14 above. Furthermore Tivoli discloses the method wherein said searching step comprises the steps of: retrieving an entry from the protected objects database; comparing the name of the database entry to the name of the system resource that is an object of the access attempt; when there is a match between the database entry and the system resource name that is the object of the access attempt, determining whether the resource is named in a symbolic link that is listed in the protected object database; and generating a list containing the exact found entry, when the entry is not named in a symbolic link listed in the protected object database. [page 19, reference "File System Aliases" up to page 22 second paragraph] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects. The governing authorization policy could be the one which are attached on the symbolic links pointing to the target resource or the authorization policy attached to the target resources directly as explained on page 19, reference "File System Aliases" up to page 22 second paragraph. All authorization policies which are attached to the symbolic links which are pointing to the target resources are checked before access to the target resource is granted and meets the recitation of this limitation.)

16. **As per claims 9, 21 and 28 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claims 1, 20 and 23 above. Furthermore Tivoli discloses the method wherein said searching step comprises the steps the method as described in claim 1 further comprising before said retrieving step the step of generating a protected objects database. [Page 9, reference "protected object Policies"; page 19, reference "File System Aliases" up to page 22 second paragraph] (As explained under the title "Protected Object Policies", on page 9, objects which are protected are stored in the protected objects database and access is granted based on the authorization police attached to these objects. The governing authorization policy could be the one which are attached on the symbolic links pointing to the target resource or the authorization policy attached to the target resources directly as explained on page 19, reference "File System Aliases" up to page 22 second paragraph)

17. **As per claims 10, 11 and 12 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claim 9 above. Furthermore Tivoli discloses the method comprising the steps of: retrieving file attributes for a system resource file; determining from said retrieved file attributes whether said resource file is a symbolic link file; when resource file is a symbolic link, retrieving the name and attributes of the system resource named in the symbolic link; and adding the symbolic link and system resource named in the symbolic link to the protected objects database. [Page 9, reference "protected object Policies"; page 19, reference "File System Aliases" up to page 22 second paragraph]

18. **As per claims 26-27 Tivoli discloses** the method for controlling access to a computing system resource, being accessed through a symbolic link file, with an externally stored resource as applied to the claim 25 above. Furthermore Tivoli discloses the method further comprising the step of denying the creation attempt when the decision component denies the creation attempt based on the security policies that govern all entries in the database protecting the system resource.[Page 9, reference "protected object Policies"; page 19, last paragraph-page 22 second paragraph]

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L

01/04/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100